IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA, Plaintiff, vs. MARK RINGLAND, Defendant.	8:17CR289 GOVERNMENT'S SUPPLEMENTAL BRIEF IN OPPOSITION TO DEFENDANT'S MOTIONS TO SUPPRESS

Prepared and Submitted by:

JOSEPH P. KELLY
United States Attorney

and

MICHAEL P. NORRIS (#17765)
Assistant U.S. Attorney
1620 Dodge Street, Suite 1400
Omaha, NE 68102-1506
(402) 661-3700

ARGUMENT

I. The Private Search Doctrine

Recently, the Fifth Circuit Court of Appeals issued a published opinion affirming the district court's denial of a motion to suppress where: 1) the defendant uploaded child pornography to a Microsoft SkyDrive account; 2) Microsoft identified the uploaded files as child pornography using PhotoDNA; 3) Microsoft sent a CyberTipline report to the National Center for Missing and Exploited Children (NCMEC) and as a result; 4) a local police officer who received the cyber report opened and viewed the uploaded files; and 5) thereafter, sought and obtained a search warrant for the residence. United States v. Reddick, ___ F.3d___, 2018 WL 3949510 at *2 (5th Cir. Aug. 17, 2018). The facts presented in Reddick are directly on point with the situation presented by Ringland. Citing the Supreme Court's decision in United States v. Jacobsen, 466 U.S. 109 (1984), and distinguishing the Tenth Circuit's decision in United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016), the Fifth Circuit held that the officer's examination of the files caused "no significant expansion of the search" that Microsoft (a private party) had already conducted, and merely "dispelled any residual doubt about the contents of the files" (which the court likened to the decision to field test the white powder in Jacobsen for controlled substances). Reddick, at *3. The Fifth Circuit went on to note that the government "effectively learned nothing from [the officer's] viewing of the files that it had not already learned from the private search." Id. at *4. Therefore, under the Private Search Doctrine, "The government did not violate Reddick's Fourth Amendment rights." Id.

"One touchstone of our Fourth Amendment jurisprudence is that the Constitution secures the right of the people against unreasonable searches and seizures conducted by the government-not searches and seizures conducted by private parties. Under the Private Search Doctrine, the

Fourth Amendment is not implicated where the government does not conduct the search itself, but only receives and utilizes information uncovered by a search conducted by a private party." Reddick at p. *1. Like Reddick, the Private Search Doctrine decides this case.

In Reddick, Microsoft, a private company, determined that the hash values of files uploaded by Reddick corresponded to the hash values of known child pornography images. Microsoft then sent CyberTips to NCMEC based on the hash values of files that Reddick had uploaded to his Microsoft account. Based on location data derived from the IP address information accompanying the files, NCMEC subsequently forwarded the CyberTips to the Corpus Christi Police Department. Upon receipt of the CyberTips, the police department viewed the suspect files, confirmed that they contained child pornography, and applied for and received a warrant to search Reddick's home and seize his computer and other devices. The search uncovered additional evidence of child pornography in Reddick's possession. Id.

In the present case, Google, a private company, determined that the hash values of files of known child pornography images were uploaded to or otherwise stored on their platform by Ringland. Google passed this information on to law enforcement through NCMEC. NCMEC forwarded the multiple CyberTips to the Nebraska State Patrol who, in turn, made them available to Investigator Alberico. Investigator Alberico viewed only those images that Google indicated to NCMEC were viewed by a human reviewer concurrent to or immediately preceding the report to NCMEC. Investigator Alberico did not conduct a separate search. She relied solely on those files clearly marked as being reviewed by Google prior to being sent to NCMEC when applying for the warrants at issue.

Under the Private Search Doctrine, 'the critical inquiry under the Fourth Amendment is whether the authorities obtained information with respect to which the defendant's expectation of

privacy has not already been frustrated." Id. at p. 2. In United States v. Jacobsen, 466 U.S. 109 (1984), a Federal Express employee observed a package that had been damaged while in transit. They opened the package and observed a white powder. They contacted the Drug Enforcement Administration. DEA agents conducted a field test on the powder which was positive for cocaine. The government then used the test results to obtain a warrant and arrest the package's intended recipients. The Supreme Court held that the agents' actions did not violate the Fourth Amendment. "Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information." Id. at 117. Any expectation of privacy the recipients had in the contents to the package was abrogated once Federal Express employees opened and searched the package discovering the white powder.

Using Jacobsen as a guide, the Fifth Circuit found that when Reddick uploaded files to his Microsoft SkyDrive, Microsoft's PhotoDNA program automatically reviewed the hash values of those files and compared them against an existing database of known child pornography hash values. "In other words, his 'package' (that is, his set of computer files), was inspected and deemed suspicious by a private actor. Accordingly, whatever expectation of privacy Reddick might have had in the hash values of his files was frustrated by Microsoft's private search." Reddick at p. 3. Thus, when the police detective opened the files, files that Microsoft had already identified as contraband, there was no "significant expansion of the search that had been conducted previously by a private party sufficient to constitute a separate search." Id. The officer's visual review of the suspect images "merely dispelled any residual doubt about the contents of the files-was akin to the government agents' decision to conduct chemical tests on the white powder in Jacobsen." Id. at p. 4.

The Fifth Circuit then proceeded to distinguish the Tenth Circuit's decision in United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016). The Court noted that in Ackerman, an investigator conducted a search of an email and three attachments who's values did not correspond to known child pornography images. Ackerman at 1306. The Fifth Circuit contrasted the facts in Reddick, similar to the facts at bar, by noting that the detective reviewed *only* those files who's hash values corresponded to the hash values of known child pornography images, as ascertained by the PhotoDNA program. His review did not sweep in any "(presumptively) private correspondence that could have contained much besides potential contraband." Reddick, at pp. 3—4. Investigator Alberico limited herself even further by only viewing those images designated as reviewed by a human at Google rather than viewing the images submitted via PhotoDNA.

II. Google's End User Agreement

Google's Terms of Service is readily available on the internet. https://policies.google.com/terms. (Ex. 1). The Terms of Service warns users not to misuse the service. "You may use our Services only as permitted by law, including applicable export and re-export control laws and regulations." (Ex. 1 at p. 1). Users are cautioned that Google "may review content to determine whether it is illegal or violates our policies, and we may remove or refuse to display content that we reasonably believe violates our policies or the law." Id. at p. 2. Users are further cautioned that "when you upload, submit, store, send or receive content to or through our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Serves), communicate, publish, publicly perform, publicly display and distribute such conduct. … our

automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored." Id. at p. 4. Google's Terms of Service, which a user such as Ringland must accept as part of registering a Google Account, prohibit Google's Services from being used in violation of law. (Ex. 2, Declaration of Cathy A. McGoff at ¶ 3).

Ringland argues that Google's actions in scrubbing more than 1,000 child pornography images from Ringland's accounts on their platform somehow transformed simple CyberTips into a governmental intrusion. He is wrong. His argument neglects Google's strong business interest in enforcing their Terms of Service and ensuring that their products are free of illegal content, in particular, child sexual abuse material. (Id. at ¶ 4). Google, like other ESPs, take steps to monitor their platform and prevent its product as being seen as a repository for abusive content involving the sexual abuse of children. Scrubbing their platform of child exploitation material preserves both their brand and business interests. Id. There is nothing sinister about an ESP policing its platform, and upon finding images of child pornography, searching other associated accounts. The sheer volume of CyberTips and the more than 1,000 files forwarded as a result of those tips, is a reflection of Ringland's desire to search for and build a library of child exploitation materials and nothing more.

Google uses its own proprietary hashing technology to tag child sexual abuse images. Each offending image, after it is viewed by at least one Google employee, is given a digital fingerprint and added to Google's repository of hashes of child pornography as defined in 18 U.S.C. § 2256. Google then uses PhotoDNA, a technology for hash matching licensed by Microsoft. (Id. at ¶ 5).

Hash values are "an algorithmic calculation that yields an alphanumeric value for a file." United States v. Stevenson, 727 F.3d 826, 828 (8th Cir. 2013); Reddick at p. 1. Hash values are used to compare the contents of two files against each other. "Hash values have been used to fight child pornography distribution, by comparing the hash values of suspect files against a list of the hash values of known child pornography images currently in circulation. This process allows potential child pornography images to be identified rapidly, without the need to involve human investigators at every stage." Reddick at p. *2.

Google, upon submitting a CyberTip to NCMEC includes a statement as to whether an image was viewed or reviewed by Google. That statement refers to a view of that image by a human reviewer concurrent to or immediately preceding the report. (Ex. 2 at ¶ 9). It is these images reviewed by Investigator Alberico and referenced in her affidavits.

Investigator Alberico only reviewed those images in which Google had undertaken a manual, human review to confirm that the image contained child pornography. She limited her viewing for purposes of obtaining the search warrants to that subset of images. The remaining images, not viewed by Investigator Alberico, would have been sent to NCMEC by PhotoDNA. Therefore, had Investigator Alberico viewed the totality of the files submitted to NCMEC through the CyberTips, her action would not violate the Fourth Amendment as the hash values had been obtained through a private search.

Google is not a government entity. Ackerman does not suggest that an initial search by an ISP is anything other than a private search. In United States v. Drivdahl, which involved a CyberTip generated by Google and sent to NCMEC, the court found that neither Google nor its investigating employee were government actors; additionally the court heard testimony that Google "has a strong business interest in ensuring that its products are free of materials depicting

child sexual abuse, and that eradicating such materials is 'critically important to protecting our users, our product, our brand, and our business interests.'" No. CR 13-18-H-DLC, 2014 WL 896734, at *4 (D.Mont. Mar. 6, 2014).

III. Good Faith Exception

Even if the court should find there was not probable cause, the good faith exception still applies here. Pursuant to the good faith doctrine, evidence obtained from an invalidated search warrant will only be suppressed if:

> (1) the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth;
> (2) the issuing magistrate wholly abandoned his judicial role;
> (3) the "affidavit [was] so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; or
> (4) the officer had no reasonable grounds for believing that the warrant was properly issued.

United States v. Leon, 468 U.S. 897 (1984); United States v. Cannon, 703 F.3d 407, 412 (8th Cir. 2013). In our case, none of these exceptions apply, and thus the evidence should not be suppressed. The defense has not asserted that the magistrate was misled, nor that he abandoned his judicial role. Nor has the defense put forth any basis for why it would be "unreasonable" for the officers to have relied on the warrant. And furthermore, based on the facts alleged in the warrant affidavit, there can be is no reasonable assertion that the affidavit was so lacking in indicia of probable cause as to render belief in its existence unreasonable. For these reasons, the good faith exception would apply to the instant case. In light of the fact that there was sufficient probable cause for the warrant and that, regardless thereof, the good faith exception would apply, the Motion to Suppress should be denied.

CONCLUSION

For the foregoing reasons, and for the reasons in the government's original brief in opposition to the motion to suppress, the United States respectfully submits that the Defendant's Motions to Suppress should be denied.

Respectfully Submitted,

UNITED STATES OF AMERICA,
Plaintiff

JOSEPH P. KELLY
United States Attorney
District of Nebraska

By: *s/ Michael P. Norris*
MICHAEL P. NORRIS (#17765)
Assistant U.S. Attorney
1620 Dodge Street, Suite 1400
Omaha, NE 68102-1506
Tel: (402) 661-3700
Fax: (402) 661-3084
E-mail: Michael.Norris@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on August 30, 2018, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which sent notification of such filing to all registered participants. I also hereby certify that a copy of the same was served by regular mail, postage prepaid, to the following non-CM/ECF participants: NONE.

s/ Michael P. Norris
Assistant U.S. Attorney